Update your Known_Hosts file to access MIT GitHub Enterprise

Update your Known_Hosts file to access MIT GitHub Enterprise

Context

Friday, September 23, 2016: A CRITICAL issue has been identified for all 2.x versions of GitHub Enterprise.

- IS&T has updated our GitHub Enterprise to the latest version to address this risk.
- At 3pm this afternoon, IS&T updated the SSH Host Keys.
- When IS&T updates the SSH Host Keys, MIT users will see a warning of a man-in-the-middle-attack. This is expected behavior.
- To resolve the warning, remove the entry for github.mit.edu from your known_hosts file.
- There might be 2 entries in the known_hosts file: one for github.mit.edu and one for 18.9.44.24
- The next time you make an SSH connection to your repository, verify that the host key fingerprint matches the fingerprint for our GitHub Enterprise host keys. Then accept the host key fingerprint.
- Detailed instructions are available below.

Step one: Remove the old key from your known hosts file.

Mac OS X or Linux users

- At a Terminal prompt, the following command will remove `-R` the `github.mit.edu` host key fingerprint.

```
ssh-keygen -R github.mit.edu
ssh-keygen -R 18.9.44.24
```

Windows users

- Launch **Notepad**
- Using Notepad, open this file:

```
C:\Users\[username]\.ssh\known_hosts
```

- Look for an entry that contains `github.mit.edu` or `18.9.44.24`. Delete the string containing `github.mit.edu`.
- Save and close the known_hosts file.

Step two: Verify that the key fingerprint matches MIT's GitHub Enterprise host key fingerprint

- The next time that you make an SSH connection to your Git repository, you will see a prompt to verify the host key fingerprint.
- You may see any of the following, depending on the configuration of your system. MIT's Enterprise GitHub host key fingerprints are:

```
1024 6a:b9:7a:75:7a:c7:4b:c2:cf:34:8e:37:4a:16:dc:b1 (DSA)

256 ac:6f:99:33:8f:9e:63:c5:4d:8f:c8:3d:b7:cd:05:b5 (ECDSA)

256 3f:9c:18:6f:be:b8:5a:bb:71:bf:be:53:c9:58:b4:13 (ED25519)

2048 03:3b:72:d6:20:6f:3e:1f:5e:2f:38:a2:80:01:f3:22  (RSA)

256 mP1vMrsRkP6l42bs0dsXejq3YgxMD2r5NqboImqssw0 (EDCSA)

2048 qtLpZn5Gd9N92Tk/9J8XoRjBh49py4/Q2xC3cV6tV2g (RSA)
```

Step three: Accept the new host key fingerprint

```
RSA key fingerprint is 03:3b:72:d6:20:6f:3e:1f:5e:2f:38:a2:80:01:f3:22.

Are you sure you want to continue connecting (yes/no)? yes
```

- Hit **Enter** to accept.
- Confirmation message will be displayed

  ```
  Warning: Permanently added 'github.mit.edu,18.9.44.24' (RSA) to the list of known hosts.
  ```

- You're done.

What will the warning message look like before I update my known_hosts file?

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the ECDSA key sent by the remote host is
SHA256:seFT9eIOmAZWbfcO9yU1sXiEYIqcrdi0qttbtmNm0Io.
Please contact your system administrator.
Add correct host key in ~/.ssh/known_hosts to get rid of this message.
Offending ECDSA key in ~/.ssh/known_hosts:42
ECDSA host key for [github.mit.edu]:122 has changed and you have requested strict checking.
Host key verification failed.
```

For more information

- See Testing your SSH Connection on GitHub Help